RÅDET FOR DIGITAL SIKKERHED

Information og anbefalinger nr. 2

Unødvendig personregistrering i nyt digitalt system til indsamling af vælgererklæringer

17. marts 2014

Resumé

Med et aktuelt lovforslag fra Økonomi- og Indenrigsministeriet (L124) planlægger regeringen at etablere et elektronisk system til registrering af vælgererklæringer i forbindelse med opstilling af politiske partier til folketinget. Som lovforslaget er udformet, vil der fremover elektronisk blive registreret oplysninger vedrørende borgeres politiske forhold. Der er i lovforslaget lagt op til dispensation fra persondataloven vedrørende registrering af personhenførbare oplysninger, selv om dette kan undgås ved anvendelse af eksisterende privatlivs-sikrende teknologi. Rådet for Digital Sikkerhed vurderer, at valget af teknologi vil have betydning for vælgernes tryghed i forhold til, hvordan registrering af oplysninger om deres politiske forhold kan anvendes.

Anbefaling

Rådet for Digital sikkerhed anbefaler at:

- Det digitale system til registrering af vælgererklæringer opbygges, så der ikke sker registrering af personhenførbare oplysninger om politiske forhold.

Baggrund

Folketinget behandler i marts 2014 et lovforslag (L124) om digitalisering af proceduren for indsamling af vælgererklæringer mv. Vælgererklæringer anvendes, når et nyt parti ønsker at stille op til Folketingsvalg eller valg til Europaparlamentet.

Lovforslaget er fremsat af Økonomi- og Indenrigsminister Margrethe Vestager. Det fremgår af bemærkningerne, at der, i det digitale system som Økonomi- og Indenrigsministeriet vil stille til rådighed for indsamling af digitale vælgererklæringer, vil ske en registrering af borgernes politiske forhold. En sådan registrering vil være i strid med Persondatalovens §7, stk. 8, som fastslår, at der ikke for den offentlige forvaltning må føres edb-registre med oplysninger om politiske forhold, som ikke er offentligt tilgængelige. Det fremgår af lovforslagets bemærkninger at der derfor administrativt vil blive fastsat hjemmel til en undtagelse fra Persondataloven, jfr. denne lovs §2, stk. 1.

Det hedder i bemærkningerne til lovforslaget, at "det er nødvendigt at fravige persondatalovens §7, stk. 8 for at muliggøre indsamlingen af vælgererklæringer ved anvendelse af et digitalt system, som Økonomi- og Indenrigsministeriet skal være overordnet ansvarlig for" og begrundelsen for at fravige anføres som "tungtvejende".

Rådet for Digital Sikkerhed vil med denne *Information og Anbefalinger* oplyse, at det er muligt ved hjælp af kendt teknologi at opbygge det digitale system, så der ikke sker en registrering af personers politiske forhold.

Information og vurderinger

Gennem de seneste år er der sket en rivende udvikling i anvendelse af krypteringsteknologier. En retning inden for denne udvikling er de såkaldte privatlivs-sikrende teknologier, som giver muligheder for at kunne arbejde med identiteter, uden at disse bliver kendt. Anvendelse af sådanne privatlivs-sikrende teknologier åbner muligheder for at undgå registrering af persondata, hvor det ikke er nødvendigt.

Vælgererklæringer kan efter Rådets vurdering digitaliseres, så ordningen skaber både nødvendig sikkerhed og indsigt hos forvaltningen og giver beskyttelse af borgernes data. Det kan ske ved anvendelse af den nævnte type teknologi.

Behovet for registrering knytter sig alene til optælling af antallet af gyldige vælgererklæringer. Derudover består der et kontrolbehov i forhold til at sikre, at de vælgere, der har afgivet erklæringer er berettigede til det.

Et digitalt system til indsamling og optælling af vælgererklæringer skal således kunne:

- skabe sikkerhed for at en vælgererklæring er afgivet af en borger, som er berettiget hertil,
- optælle hvor mange vælgererklæringer, der er afgivet,
- sikre anonymitet for de borgere, der har afgivet vælgererklæringen, så deres politiske forhold ikke registreres.

Lovforslaget indeholder nogle supplerende krav, som naturligvis skal medtages i opbygningen af det digitale system.

En klassisk løsning (og den der er lagt op til fra ministeriet) vil være at opbevare afgivne vælgererklæringer i en krypteret database og dekryptere disse data, når de skal bruges, f.eks. når antallet af vælgererklæringer skal valideres og optælles. Der er flere problemer ved denne løsning. Borgerne har blandt andet ingen garanti for, at data ikke bliver dekrypteret i andre tilfælde end ved selve optællingen/valideringen, og data kan lækkes under eller efter denne optælling/validering.

Det findes allerede i dag løsninger, som vil kunne realisere digitale vælgererklæringer uden disse problemer. Det er teknologier, der lever op til den kommende persondataforordning fra EU på områder som "privacy by design". Rådet for Digital Sikkerhed kan i samarbejde med Alexandra Instituttet umiddelbart skitsere to forslag til metoder, der begge vil kunne implementeres som en service, hvor borgeren logger ind med NemID og i ét flow genererer og afgiver en vælgererklæring, uden at oplysninger om, hvilken borger der er tale om, siden vil kunne afkodes.

Brug af pseudonym via token

Denne metode er kendt under navnet privacy Attribute Based Credentials (pABC), og den fungerer som en speciel anonymiseret version af digitale signaturer. Metoden kendes blandt andet fra Microsoft U-Prove og IBM Identity Mixer. Hvis der bruges pABC, vil borgeren, når han/hun vil støtte et parti, skulle logge på en service med NemID og generere et pseudonymiseret digitalt token. Det kan sammenlignes med en anonym 'billet', hvis ægthed kan verificeres af en 'kontrollør'. Dette token vil af borgeren (via vedkommendes computer) blive sendt til databasen over vælgererklæringer, hvor det vil blive valideret anonymt, at borgeren ikke har givet vælgererklæring før, og at borgeren ikke har trukket sin erklæring tilbage (hvis mulighed for tilbagetrækning af erklæringer ønskes).

Sikker validering via flere parter

En anden muligt metode er kendt under navnet sikre flerpartsberegninger (Multi Party Computation, MPC). Denne metode er baseret på beregninger på krypterede data, uden at de underliggende data kan afkodes. Løsninger af denne type er kommercielt i brug i dag, blandt andet udbudt af et antal danske virksomheder. I en sådan løsning vil borgeren også logge ind på en service ved hjælp af NemID. Borgeren genererer en digital vælgererklæring, som bliver krypteret og sendt til både Indenrigsministeriet og det opstillende parti på en måde, så ingen af

de to parter kan dekryptere oplysning om hvilken borger der har afgivet erklæringen. Til gengæld kan både Indenrigsministeriet og partiet ved hjælp af software, der kan installeres på en almindelig computer, udføre en beregning på de krypterede data. Denne beregning vil i dette tilfælde være en optælling/validering af erklæringerne, foretaget sådan at persondata aldrig bliver dekrypteret, hverken før, under eller efter optællingen. Det eneste der bliver dekrypteret er resultatet, altså hvor mange valide erklæringer partiet har modtaget.

Begge teknologier vil kunne benyttes til det nye system for elektronisk indsamling af vælgererklæringer, og for den almindelige borger vil det ikke være tydeligt, hvilken der er brugt. Rådet vil ikke på nuværende tidspunkt anbefale den ene løsning frem for den anden. Vi har beskrevet begge teknologier for at vise, at der findes forskellige eksisterende løsninger, som kan sikre at oplysninger om borgernes politiske forhold holdes hemmelige.

Det er Rådets vurdering, at digitaliseringen af vælgererklæringer er en eksemplarisk opgave i forhold til anvendelse af privatlivs-sikrende teknologi, da den er velafgrænset og har et overskueligt omfang i drift. Endvidere vil de foreslåede løsninger opfylde kravene om 'privacy by design' i den kommende EU-forordning om databeskyttelse.

Der er efter Rådets vurdering ingen tvivl om, at et digitalt system baseret på de ovenfor beskrevne privatlivs-sikrende teknologi vil være en administrativ forenkling og samtidig også give en lettere opstillingsprocedure for ny partier. Anvendelse af de beskrevne teknologier kan derudover realiseres i et system, som er brugervenligt for borgerne.

Rådet vurderer således at det ikke er nødvendigt at fravige Persondatalovens §7, stk. 8's forbud mod edb-registrering af politiske forhold. Dette vurderer Rådet i sig selv som en selvstændig tilstrækkelig begrundelse for opbygning af et digitalt system med anvendelse af privatlivs-sikrende teknologi. Rådet kan dermed ikke tilslutte sig, at der skulle være tale om en 'tungtvejende' grund til at fravige Persondatalovens gældende bestemmelser.

Rådet vurderer også, at en privatlivs-sikrende teknologi vil reducere risikoen for, at nogle vælgere undlader at afgive en vælgererklæring til støtte for opstilling af et nyt parti på grund af utryghed i forhold til, hvordan registreringen af oplysninger om deres politiske forhold kan opbevares og anvendes.

Endelig anser Rådet det for vigtigt at der i den hastige digitalisering af borgernes kontakt med offentlige myndigheder og andre digitale systemer er stor opmærksomhed på, at hensynet til borgernes privatliv og it-sikkerhed integreres i it-systemer til håndtering af data om borgerne. Et digitalt system for indsamling og optælling af vælgererklæringer er efter Rådets opfattelse et godt eksempel på, hvordan en tilgængelig løsning kan fremme borgernes privatlivsbeskyttelse uden at forringe kvaliteten og sikkerheden af de data, som er nødvendige for at sikre kontrol med afgivne vælgererklæringer.

Om Rådet for Digital Sikkerhed

Med mere end 45 medlemsorganisationer arbejder Rådet for Digital Sikkerhed for at skabe fokus på tryg digitalisering. Vi bidrager med viden og analyser, som kan være med til at sætte retningen for fremtidens digitale velfærdssamfund. Rådet arbejder for at it-sikkerhed og privatlivsbeskyttelse bliver naturligt integreret i systemer og samfund. Rådet vil understøtte læring og sund adfærd i den digitale verden samt innovativ udnyttelse af teknologiens muligheder.

Yderligere information: www.digitalsikkerhed.dk